

REMARKS

Claims 1, 18, 24, 27, 39, 42 and 57 have been amended to improve and claims 19 and 29 have been canceled without prejudice or disclaimer. Claims 1-7, 10, 12-18, 21-25, 27, 31-33, 35, 37-46, 49, 50 and 52-69 are now pending in this application.

Claims 24, 27, 39, 42 and 57 have been rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Claims 24, 27, 39, 42 and 57 have hereby been amended and are now believed to more clearly define statutory subject matter. For example, claim 24, as amended, recites at least one processing device configured to execute the TCP reassembly software module, the software module for inspecting the TCP stream, the software module for dropping a TCP packet and the software module for forwarding a TCP packet. Claims 27, 39, 42 and 57 have been similarly amended and now recite more than a series of software modules.

Accordingly, withdrawal of the rejection of claims 24, 27, 39, 42 and 57 under 35 U.S.C. § 101 is respectfully requested.

Claims 1-7, 10, 12-18, 21-25, 27, 31-33, 35, 37-41, 43-45, 49-50, 52-56, 58 and 60-69 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,499,107; hereinafter Gleichauf '107) and Gleichauf et al. (U.S. Patent No. 6,324,656; hereinafter Gleichauf '656) in view of Nikander et al. (U.S. Patent No. 6,253,321; hereinafter Nikander) and further in view of Copeland III (U.S. Patent Application Publication No. 2003/0105976; hereinafter Copeland III); claims 19 and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf '107 and Gleichauf '656 in view of Nikander and Copeland III and further in view of Alexander et al. (U.S. Patent Publication No. 2004/0258073; hereinafter Alexander); and claims 42, 46, 57 and 59 have been rejected under

35 U.S.C. § 103(a) as being unpatentable over Gleichauf '107 in view of Nikander and further in view of Trcka et al. (U.S. Patent No. 6,453,345; hereinafter Trcka). The rejections are respectfully traversed.

Initially, the applicants note that claims 42 and 57 have been rejected based on the combination of Gleichauf '107, Nikander and Trcka. Claims 43-45, 49, 50, 52-55, 58, 60 and 63-69, which variously depend on claims 42 and 57, have been rejected based on the combination of Gleichauf '107 and Gleichauf '656 in view of Nikander. This inconsistency was pointed out in the last response, but has not been addressed. In any event, the rejection of these dependent claims (i.e., claims 43-45, 49, 50, 52-55, 58, 60 and 63-69) is not consistent with the rejection of independent claims 42 and 57. The applicants once again respectfully request clarification as to the grounds of rejection in any subsequent communication.

Claim 1 recites that the method includes grouping the plurality of TCP packets into packet flows and sessions and storing the packet flows in packet flow descriptors. Claim 1 also recites that the inspecting the TCP stream to detect information indicative of a security breach comprises searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream. Claim 1, as amended, further recites that the packet flow descriptors are addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type. A similar feature was previously recited in claim 19 and therefore the applicants will address claim 1 in a manner consistent with the rejection of claim 19 in the Office Action (which included the Alexander reference).

As to the feature previously recited in claim 19, the Office Action admits that none of Gleichauf '107, Gleichauf '656, Nikander or Copeland III discloses this feature (Office Action

– page 13). The Office Action, however, states that Alexander discloses computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type and points to Alexander at page 3, paragraph 27 for support (Office Action – page 13).

Alexander discloses that mapping function services 230 performs a hash function on the 5-tuple for the purpose of performing multi-protocol label switching (Alexander – Abstract and paragraphs 24-27). Alexander is not at all related to detecting security breaches by storing packet flows in packet flow descriptors that are addressed by a hash value computed from a source IP address, a destination IP address, a source port, a destination port and a protocol type, as required by claim 1. Alexander, therefore, cannot further disclose searching for a network attack identifier in a TCP stream based on the packet flow descriptors and sessions associated with the TCP stream, as further required by amended claim 1. In contrast, Alexander merely discloses using a mapping function for performing MPLS switching.

For at least these reasons, the combination Gleichauf '107, Gleichauf '656, Nikander, Copeland III and Alexander does not disclose or suggest each of the features of claim 1.

In addition, even if, for the sake of argument, the combination of these five references could be construed to disclose or suggest each of the features of claim 1, the applicants respectfully assert that the motivation to combine these five references does not satisfy the requirements of 35 U.S.C. § 103.

For example, as discussed above, Alexander is not at all related to detecting security breaches and is not at all related to the other four references. The Office Action states that it would have been obvious to combine Alexander with Gleichauf '107, Gleichauf '656, Nikander and Copeland III “so as to effectively performing packet filtering” (Office Action –

page 13). This alleged motivation is merely a conclusory statement providing an alleged benefit of the combination. Such motivation does not satisfy the requirements of 35 U.S.C. § 103. In addition, the applicants note that no portion of any of the references is pointed to as providing objective motivation for combining Alexander, which is directed to load sharing in an MPLS system, with the combination of the other four references. The applicants respectfully assert that it would not have been obvious to combine these unrelated references absent impermissible hindsight.

For at least the reasons discussed above, withdrawal of the rejection and allowance of claim 1 are respectfully requested.

Claims 2-7, 10, 12-17, 21 and 23 depend from claim 1 and are believed to be allowable for at least the reasons claim 1 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 2-7, 10, 12-17, 21 and 23 are respectfully requested.

Claims 18, 24 and 27, as amended, recite features similar to, but of different scope than claim 1. For reasons similar to those discussed above with respect to claim 1, withdrawal of the rejection and allowance of claims 18, 24 and 27 are respectfully requested.

Claims 25, 31, 33, 35, 37, 38, 40 and 41 depend from claim 24 and are believed to be allowable for at least the reasons claim 24 is allowable. Claim 32 depends from claim 27 and is believed to be allowable for at least the reasons claim 27 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 25, 31-33, 35, 37, 38, 40 and 41 are respectfully requested.

Claim 22 recites querying a signatures database to determine whether there are matching signatures in the TCP stream using deterministic finite automata for pattern matching. Claim 39 recites a similar feature. The Office Action admits that Gleichauf '107,

Gleichauf '656 and Nikander do not disclose these features, but takes Official Notice that employing "use of deterministic finite automaton for providing a pattern matching is well known in the theory of computation" (Office Action – page 11). The applicants, however, note that claims 22 and 39 recite more than just a generic use of pattern matching using deterministic finite automata. For example, claim 22 recites querying a signatures database to determine whether there are matching signatures in the TCP stream using deterministic finite automata for pattern matching. Therefore, the mere fact that deterministic finite automata techniques are known, in general, does not mean that they are well known in the manner recited in claims 22 and 30. In response to a similar argument regarding the use of Official Notice, the, Office Action cites two documents (listed on the PTO-892 accompanying the Office Action and referred to herein as Navarro 1997 and Navarro 1998) that allegedly disclose the use of deterministic finite automata (DFA) (Office Action – page 3). Once again, the applicants note that Navarro 1997 and Navarro 1998 may generally disclose DFA techniques. These documents, however, do not disclose the use of DFA in the manner recited in claims 22 and 39. The applicants respectfully request that any subsequent communication particularly point to which portions of Navarro 1997 or Navarro 1998 allegedly disclose the claimed features or withdraw the rejection.

For at least these reasons, the combination of Gleichauf '107, Gleichauf '656 and Nikander does not disclose or suggest each of the features of claims 22 and 39. Accordingly, withdrawal of the rejection and allowance of claims 22 and 39 are respectfully requested.

Claims 42, 46, 57 and 59 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf '107 in view of Nikander and further in view of Treka. The rejection is respectfully traversed.

Claims 42 and 57, as amended, recite features similar to, but not identical to claim 1.

For reasons similar to those discussed above with respect to claim 1, the combination of Gleichauf '107 and Nikander does not disclose each of the features of amended claims 42 and 57. In addition, none of Trcka, Copeland III or Alexander remedies the deficiencies in the combination of Gleichauf '107 and Nikander discussed above with respect to claim 1. Accordingly, withdrawal of the rejection and allowance of claims 42 and 57 are respectfully requested.

Claims 46 and 59 are dependent on claims 42 and 57, respectively, and are believed to be allowable for at least the reasons claims 42 and 57 are allowable. Accordingly, withdrawal of the rejection and allowance of claims 46 and 59 are respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, the applicants respectfully request withdrawal of the outstanding rejections and the timely allowance of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /Glenn Snyder/
Glenn Snyder
Reg. No. 41,428

Date: January 17, 2007

11350 Random Hills Road
Suite 600
Fairfax, VA 22030
Telephone: (571) 432-0800
Facsimile: (571) 432-0808